(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 293 456 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
20.12.2023 Bulletin 2023/51

(21) Application number: **22178672.6**

(22) Date of filing: **13.06.2022**

(51) International Patent Classification (IPC):
G05B 23/02 *(2006.01)* ***G06Q 10/00*** *(2023.01)*

(52) Cooperative Patent Classification (CPC):
G06Q 10/20; G05B 23/0283

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(71) Applicant: **ABB SCHWEIZ AG**
5400 Baden (CH)

(72) Inventors:
- **GRUENER, Sten**
  69514 Laudenbach (DE)
- **PLATENIUS-MOHR, Marie Christin**
  69493 Hirschberg an der Bergstraße (DE)
- **TROSTEN, Anders**
  724 76 Västerås (SE)

(74) Representative: **Maiwald GmbH**
Engineering
Elisenhof
Elisenstrasse 3
80335 München (DE)

(54) **METHOD AND SYSTEM FOR ANONYMIZATION AND NEGOTIATION FOR PREDICTIVE MAINTENANCE**

(57) A method for anonymization and negotiation for predictive maintenance, the method comprising: Aggregating (S11), by an aggregation service module (110), runtime data and/or context data using an aggregation policy to generate aggregated data; Anonymizating (S12), by an anonymization module (120), the aggregated data using a user-definable internal anonymization policy to generate anonymized data; and Sending (S13), by a transmitting module (130), the anonymized data to a condition prediction service module (210).

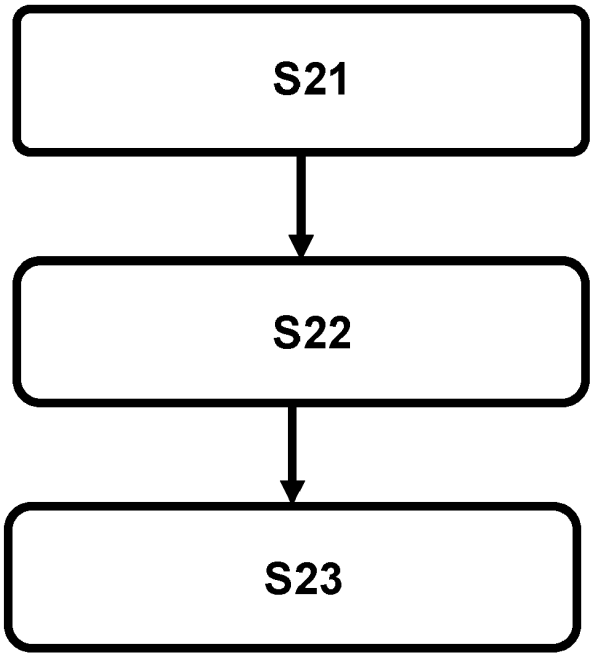

Fig. 4

EP 4 293 456 A1

Description

TECHNICAL FIELD

[0001] The present disclosure relates to a method and a system for anonymization and negotiation for predictive maintenance. In particular the present invention relates to methods and systems for anonymization of information and parameter negotiation for predictive maintenance.

TECHNICAL BACKGROUND

[0002] The general background of this disclosure is predictive maintaince.

[0003] Predictive maintenance applications are typical cross-company applications where different companies exchange data. For example, a plant operator (O) is owning devices and data from the physical plant and from the process these devices are attached to (e.g., temperature, pressure etc.). The device manufacturer or maintenance company (M) has device-specific information from their experience pool (e.g., device fleet analysis across multiple operators) which may help them to identify issues with devices early. Furthermore, typically devices are operated within a technical scope on O's site, e.g. a DCS, which is provided by some automation vendor (A).

[0004] Within predictive maintenance applications, the exchanged data is sensitive as each site has reasons for limited trust towards other parties:

- O: does not want to expose too much of its process data either to M or A, e.g., due to commercial secrets of production like recipes or production volumes.
- M: does not want to expose its device knowledge to others, in order not to lose competitive advantage.
- A: as "information broker" between M and O, A is interested in a neutral role and into ensuring trust from M and O.

[0005] Current solutions for predictive maintenance suffer from the following flaws:

- Disbalance between O's and M's interests:
    - ◦ M gets "unlimited" access to O's operational data on M's devices installed on O's sites
    - ◦ M does not get any access to "context" of its devices, only the "isolated" runtime data of the devices
    - ◦ O gets the "predictive maintenance algorithm" in its physical possession, e.g. as part of device firmware, allowing possibly to tamper and extract it
- A has limited control over information flows between components in the system as they are extracted by 3rd party systems and passed outside A's infrastructure, e.g. by using side-channels like embedded 4G/5G modems, Bluetooth connectivity etc.

[0006] Fixes to those flaws are currently labor-expensive and error-prone project-specific manual work. For example, the amount and quality of exchanged information needs to be defined in a project specific way. The same holds for the mechanisms of information exchange, i.e., service invocations, authentication and the definition of the format of the exchanged information.

SUMMARY OF THE INVENTION

[0007] The present invention solves the problem of avoiding error-prone project-specific manual work. The present invention provides a method and a system for anonymization and negotiation for predictive maintenance and for (de-)anonymization of information and parameter as defined in the appended claims. Further embodiments are provided by the description.

[0008] In one aspect of the invention a method for anonymization and negotiation for predictive maintenance is provided, the method comprising the stepf of: aggregating, by an aggregation service module, runtime data and/or context data using an aggregation policy to generate aggregated data; anonymizating, by an anonymization module, the aggregated data using a user-definable internal anonymization policy to generate anonymized data; and sending, by a transmitting module, the anonymized data to a condition prediction service module.

[0009] The modules as defined in the present description of the present patent application and in particular the aggregation service module, (de)anonymization module, the condition prediction service module, the quality estimation service module may be a hardware device or a software functionatlity as also for example a digital service running on an existing device (edge device, controller. In other words, the term "module" as used and defined in the present description of the present patent application may be understood as a building block of a software system that is created during modularization, represents a functionally closed unit and provides a specific service.

[0010] The present invention advantageously provides predictive maintenance applications for which different companies exchange data e.g. an operator sends device runtime information to the device manufacturer to receive an estimation of device's condition. Currently such interactions need to be set up manually with a limited control of the exchanged information amount.

[0011] The present invention advantageously provides a system for a structured definition of information to be exchanged between companies and anonymization rules applied to this information.

[0012] The present invention advantageously allows users to have a better control of the information which is leaving their organization and having a faster i.e. cheaper setup of condition monitoring infrastructure.

[0013] According to an exemplary embodiment of the present invention, the aggregation policy is created statically or dynamically according to pre-defined rules.

[0014] According to an exemplary embodiment of the present invention, the user-definable internal anonymization policy is configured per device instance and/or asset instance or based on anonymization policy rules based on properties of the device instance and/or asset instance.

[0015] According to an exemplary embodiment of the present invention, the user-definable internal anonymization policy is configured using machine learning.

[0016] According to an exemplary embodiment of the present invention, the user-definable internal anonymization policy may contain at least one of the following anonymization rules to be applied on exchanged data: value anonymization rules, history-limit rules, identity anonymization rules, context anonymization rule.

[0017] According to an exemplary embodiment of the present invention, the method is further comprising the step of adjusting the user-definable internal anonymization policy dynamically.

[0018] According to an aspect of the present invention, a method for deanonymization and negotiation for predictive maintenance is provided, the method comprising the following steps of receiving, by a condition prediction service module, the anonymized data from a transmitting module; deanonymizating, by an deanonymization module, the received and anonymized data using a user-definable internal deanonymization policy to generate deanonymized data; and providing, by a quality estimation service module, prediction service based on the deanonymized data to generate predicition data.

[0019] According to an exemplary embodiment of the present invention, the user-definable internal deanonymization policy is configured per device instance and/or asset instance or based on deanonymization policy rules based on properties of the device instance and/or asset instance.

[0020] According to an exemplary embodiment of the present invention, the user-definable internal deanonymization policy is configured using machine learning.

[0021] According to an exemplary embodiment of the present invention, the user-definable internal deanonymization policy may contain at least one of the following deanonymization rules to be applied on exchanged data: value deanonymization rules, history-limit rules, identity deanonymization rules, context deanonymization rules.

[0022] According to an exemplary embodiment of the present invention, the method is further comprising the step of adjusting the user-definable internal deanonymization policy dynamically.

[0023] According to an aspect of the present invention a system for anonymization and negotiation for predictive maintenance is provided, the system comprising: an aggregation service module configured to aggregate runtime data and/or context data using an aggregation policy to generate aggregated data; an anonymization module configured to anonymizate the aggregated data using a user-definable internal anonymization policy to generate anonymized data; and a transmitting module configured to send the anonymized data to a condition prediction service module.

[0024] According to an aspect of the present invention a system for deanonymization and negotiation for predictive maintenance is provided, the system comprising: a condition prediction service module configured to receive the anonymized data from a transmitting module; an deanonymization module configured to deanonymizate the anonymized data using a user-definable internal deanonymization policy to generate deanonymized data; and a quality estimation service module configured to provide prediction service based on the deanonymized data to generate predicition data.

[0025] According to an aspect of the present invention a network for predictive maintenance is provided, the network comprising the system for anonymization and the system for deanonymization.

[0026] Any disclosure and embodiments described herein relate to the method and the system, lined out above and vice versa. Advantageously, the benefits provided by any of the embodiments and examples equally apply to all other embodiments and examples and vice versa.

[0027] As used herein "determining" also includes "initiating or causing to determine", "generating" also includes "initiating or causing to generate" and "provding" also includes "initiating or causing to determine, generate, select, send or receive". "Initiating or causing to perform an action" includes any processing signal that triggers a computing device to perform the respective action.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] In the following, the present disclosure is further described with reference to the enclosed figures:

Fig. 1 illustrates a static view of components and schematic information flows and anonymization of condition monitoring information according to an exemplary embodiment of the present invention;

Fig. 2 illustrates an example for interactions between user and the engineering system and UI according to an exemplary embodiment of the present invention;

Fig. 3 illustrates an method for anonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention;

Fig. 4 illustrates an method for deanonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present

invention;

Fig. 5 illustrates an system for anonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention;

Fig. 6 illustrates an system for deanonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention;

DETAILED DESCRIPTION OF EMBODIMENT

[0029] The following embodiments are mere examples for the method and the system disclosed herein and shall not be considered limiting.

[0030] Fig. 1 illustrates a static view of components and schematic information flows and anonymization of condition monitoring information according to an exemplary embodiment of the present invention.

[0031] According to an exemplary embodiment of the present invention, a set of user-configurable anonymization and deanonymization services is provided allowing to adapt runtime and context data of a monitored asset before this data is passed outside the organization.

[0032] According to an exemplary embodiment of the present invention, furthermore, structured anonymization rules allow deanonymization of external condition predictions before processing them within the organization.

[0033] According to an exemplary embodiment of the present invention, the flexibility of the system allows automatic negotiation between organizations to find an optimal tradeoff between the amount and the quality of the shared data with the quality of received predictions as it is expected that the quality/reliability of the prediction declines with the amount of anonymization that is applied to the original data.

[0034] According to an exemplary embodiment of the present invention, a system for anonymization and negotiation of predictive maintenance data and parameters is provided. This system can typically be executed on an Edge device provided by A and deployed within O's organization (this applies for services marked with "<O>" in Figure 1). The 3rd party condition prediction service (marked with "<M>" in Figure 1) does not have to fulfill any deployment requirements and can, e.g., run in M's cloud to ensure confidentiality of included algorithms.

[0035] According to an exemplary embodiment of the present invention, the cross-company communication between O and M is handled by the Caller Service and Receiver Service on O's site and the Condition Prediction Service on M's side. In order to request a maintenance suggestion, the caller service provides the runtime data (e.g., temperature, vibration, stroke count, current etc.) (arrow 6b in Figure 1) and context data (e.g., its location, its environmental condition like ambient temperature, its physical surroundings (like connection to other device types) of device(s)) (arrow 6b in Figure 1) to the Condition Prediction Service.

[0036] According to an exemplary embodiment of the present invention, the main output of the Condition Prediction Service is the Estimated Asset Condition (arrow 7b) which is received by Caller Service of O and processed further. Technical realization of service interactions is possible using interoperable semantic information containers (e.g., Asset Administration Shell -AAS) and AAS-infrastructure like registries to accomplish discovery of available condition prediction services.

[0037] According to an exemplary embodiment of the present invention, moving away from central interaction between O and M organizations, let us describe the remaining components and information flows. Before the information about device or other asset's (identification of the asset of interest is transferred via arrow 1 in Figure 1) can be sent to M, it needs to be aggregated from multiple information sources within O's infrastructure (arrows 2 and 3 in Figure 1).

[0038] According to an exemplary embodiment of the present invention, the information sources are manyfold, e.g., control systems for current device values, historian systems for historical process values (arrow 2), engineering systems for device context information like its location etc. (arrow 3).

[0039] According to an exemplary embodiment of the present invention, the aggregation is handled by the Aggregation service which processes the so-called aggregation policy to collect data (arrow I). This policy can be created statically (i.e., once) or dynamically (i.e., during the condition monitoring request) according to pre-defined rules. The static aggregation policy and rules for dynamic aggregation are defined by the user of the system via suitable engineering tools or wizards.

[0040] According to an exemplary embodiment of the present invention, in the subsequent step, a user-definable internal Anonymization Policy is processed by the Anonymization Service on O's site (I) prior to aggregated device data (arrow 4) leaving the company via the caller service (arrow 6a). The anonymization policy is created/configured manually per device/asset instance or in a rule-based fashion based on certain device's properties (e.g., its type and vendor, or its physical location) or machine learning.

[0041] According to an exemplary embodiment of the present invention, the anonymization policy may contain the following anonymization rules to be applied on exchanged data:

- Value anonymization rules
    - ◦ Adding noise to the value
    - ◦ Adding drift
    - ◦ Changing precision, e.g., rounding, flooring
    - ◦ Time-delays
    - ◦ Further parameter based rules

- History-limit rules
  - ◦ Sending only selected number of latest values of the device
  - ◦ Reducing sampling rates within the time window
- Identity anonymization rules
  - ◦ No or tampered device identification, e.g., random IDs or serials
- Context anonymization rules related to
  - ◦ Physical environment of the device (e.g., ambient temperature) + value anonymization
  - ◦ Device location anonymization
  - ◦ Tampered topology of device's installation, e.g. modification of the details regarding device neighboring systems and devices, e.g. change or simplify existing piping and electrical signal layout

[0042] An additional aspect of anonymization can involve means of homomorphic encryption allowing the Condition Prediction Service to operate on transmitted encrypted values of Caller Service without decrypting them. In particular, the homomorphic encryption can be applied for Machine Learning systems since a trained model can be broken down in a set of addition and multiplication operations, cf. patent application EP 3412000A1. As therein described, the training and the prediction may take place on encrypted data, which is processed based on homomorphic encryption. Homomorphic encryption provides the possibility that calculations may be based on plaintext data and encrypted data simultaneously. There may be one or more functions mapping a plaintext first data value and an encrypted second data value to an encrypted result data value, which are compatible with the encryption. When the result data value is decrypted, it may have the same value, as when a specific other function, such as addition or multiplication, is applied to the first data value and the encrypted second data value.

[0043] According to an exemplary embodiment of the present invention, after modifying the runtime and context, the data which is related to the device (arrow 5), is sent to the Condition Prediction Service of another party (arrow 6b). The data is complemented by an External Anonymization Policy (arrow 6a) which is disclosed to M and might be used to improve or indicate uncertainty in the prediction.

[0044] The External Anonymization Policy is not just a copy of the internal one, but again is a partially anonymized reflection of the internal policy. The amount of anonymization information, which is disclosed to the other party, is selected either manually or based on predefined rules in a semi-automated fashion.

[0045] According to an exemplary embodiment of the present invention, the Condition Prediction Service consumes provided runtime and context information including available external anonymization policy via its algorithm.

[0046] According to an exemplary embodiment of the present invention, based on this information the condition of the device is predicted, e.g. signalizing a normal or an abnormal condition of the device. The prediction (arrow 7b) is accomplished by a Prediction Quality Estimation (arrow 7a) which the Condition Prediction Service is producing based on the input information and on internal knowledge and will be used in later steps.

[0047] According to an exemplary embodiment of the present invention, the predicted condition is further processed by O's infrastructure. Here, deanonymization of results is made, if possible, by the Deanonymization Service (arrow 8). This can, for example, include changing the tampered IDs of the device which have been transmitted to M back to its proper internal Identification.

[0048] According to an exemplary embodiment of the present invention, the exchange is done continuously, e.g., in pre-defined intervals. In case that non-sufficient quality of the prediction has been indicated externally by the prediction service or detected internally by the Quality Estimation Service based on external quality estimation (arrow 9) and deanonymized prediction data (arrow 10), a specific action can be triggered.

[0049] According to an exemplary embodiment of the present invention, such actions can be and informing the user and opening a wizard to re-adjust policies, or automatic dynamic negotiation of parameters (described below). The Quality Estimation Service may use a database of previous predictions and set of internal rules to detect insufficient prediction quality.

[0050] According to an exemplary embodiment of the present invention, based on the Aggregation Policy, the predicted condition of the device a passed to the Decomposition Service (arrow 11), which dispatches the results to one or multiple Maintenance Action Sinks (arrow 12), e.g., operator display or O's maintenance system.

[0051] According to an exemplary embodiment of the present invention, along with described components, an Engineering System and UI component is part of the systems. The simplified sequence of events when interacting with the engineering system is shown in the following Fig. 2.

[0052] Fig. 2 illustrates an example for interactions between user and the engineering system and UI according to an exemplary embodiment of the present invention.

[0053] According to an exemplary embodiment of the present invention, the initial setup of condition monitoring is performed by a user, e.g., application engineer, interacting with the engineering system, by opening a wizard, selecting the Asset ID (e.g., the serial number of the device) to be monitored.

[0054] According to an exemplary embodiment of the present invention, the next step is selecting a suitable external Condition Prediction Service which is suitable

for the particular device to be monitored.

[0055] According to an exemplary embodiment of the present invention, the Condition Prediction Service supplies its meta information, e.g., information which needs to be supplied by the Caller Service.

[0056] According to an exemplary embodiment of the present invention, based on this requested information, the user uses the engineering system to browse available information sources and select the information to be exchanged with M.

[0057] According to an exemplary embodiment of the present invention, after the information amount is fixed, the anonymization is defined based on the application needs.

[0058] According to an exemplary embodiment of the present invention, the next step defines the rule set to assess whether the returned prediction suffices the application needs.

[0059] According to an exemplary embodiment of the present invention, the prediction system is started with this information.

[0060] According to an exemplary embodiment of the present invention, in case an insufficient prediction quality has been detected by the Prediction Quality Estimation Service, i.e., the acceptance rule set is violated, the user is informed and asked to re-define anonymization policies and/or acceptance rules to either increase the information respectively its quality which is provided to M or to lower the expectations of the received predictions.

[0061] According to an exemplary embodiment of the present invention, a dynamic negotiation of anonymization policy depending on the prediction quality is performed as follows:

According to an exemplary embodiment of the present invention, a possibility to adjust the anonymization policy dynamically is based on prediction quality opens an additional possibility for negotiation and dynamic adjustments of the anonymization policy either during the operation of the system or a-priori, i.e., during the setup if the condition monitoring process.

[0062] According to an exemplary embodiment of the present invention, based on collected knowledge from previous interactions, the condition prediction service may not only communicate the list of needed information about the asset, e.g. list of required parameters and variables, but also indicate which anonymization might be adequate for each parameter in order to acquire meaningful prediction results.

[0063] According to an exemplary embodiment of the present invention, such indicators may include, but are not limited to:

- Minimal resolution of information
- Minimal sampling rates of each parameter
- Required non-functional information about the device, e.g., number of hours in operation.

[0064] According to an exemplary embodiment of the present invention, a table or even a mathematical function may be included in Condition Prediction Service to indicate how the provided quality of information correlates with the prediction result quality, for example: a sampling rate of parameter X and included history of parameter X of at least 60 days will result in 90% prediction accuracy (e.g., in terms the expected F1 score of the classifier).

[0065] According to an exemplary embodiment of the present invention, the negotiation process itself can again technically be based on industry 4.0 technologies, like the Asset Administration Shell, especially on so-called "Type-3 AAS" interacting using so-called Industry 4.0 language.

[0066] Fig. 3 illustrates an method for anonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention.

[0067] A method for anonymization and negotiation for predictive maintenance comprises at least the following steps:

As a first step of the method, aggregating S11, by an aggregation service module 110, runtime data and/or context data is performed using an aggregation policy to generate aggregated data.

[0068] As a second step of the method, anonymizating S12, by an anonymization module 120, the aggregated data is performed using a user-definable internal anonymization policy to generate anonymized data.

[0069] As a third step of the method, sending S13, by a transmitting module 130, the anonymized data to a condition prediction service module 110 is performed.

[0070] Fig. 4 illustrates an method for deanonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention.

[0071] A method for deanonymization and negotiation for predictive maintenance, the method comprising:

As a first step of the method, receiving S21, by a condition prediction service module 210, the anonymized data from a transmitting module 130 is performed.

[0072] As a second step of the method, deanonymizating S22, by an deanonymization module 220, the received and anonymized data using a user-definable internal deanonymization policy to generate deanonymized data is performed.

[0073] As a third step of the method, providing S23, by a quality estimation service module 230, prediction service based on the deanonymized data to generate predicition data is performed.

[0074] Fig. 5 illustrates a system for anonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention.

[0075] A system 100 for anonymization and negotiation for predictive comprises an aggregation service module 110 configured to aggregate runtime data and/or context data using an aggregation policy to generate aggregated data.

[0076] The system 100 for anonymization and negotiation for predictive comprises an anonymization module

120 configured to anonymizate the aggregated data using a user-definable internal anonymization policy to generate anonymized data.

[0077] The system 100 for anonymization and negotiation for predictive comprises a transmitting module 130 configured to send the anonymized data to a condition prediction service module 210.

[0078] Fig. 6 illustrates a system for deanonymization and negotiation for predictive maintenance according to an exemplary embodiment of the present invention.

[0079] A system 200 for deanonymization and negotiation for predictive maintenance comprises a condition prediction service module 210 configured to receive the anonymized data from a transmitting module 130.

[0080] The system 200 for deanonymization and negotiation for predictive maintenance further comprises an deanonymization module 220 configured to deanonymizate the anonymized data using a user-definable internal deanonymization policy to generate deanonymized data.

[0081] The system 200 for deanonymization and negotiation for predictive maintenance further comprises a quality estimation service module 230 configured to provide prediction service based on the deanonymized data to generate predicition data.

[0082] In the claims as well as in the description the word "comprising" does not exclude other elements or steps and the indefinite article "a" or "an" does not exclude a plurality. A single element or other unit may fulfill the functions of several entities or items recited in the claims. The mere fact that certain measures are recited in the mutual different dependent claims does not indicate that a combination of these measures cannot be used in an advantageous implementation.

Claims

1. A method for anonymization and negotiation for predictive maintenance, the method comprising:

   - Aggregating (S11), by an aggregation service module (110), runtime data and/or context data using an aggregation policy to generate aggregated data;
   - Anonymizating (S12), by an anonymization module (120), the aggregated data using a user-definable internal anonymization policy to generate anonymized data; and
   - Sending (S13), by a transmitting module (130), the anonymized data to a condition prediction service module (210).

2. The method according to claim 1,
   wherein the aggregation policy is created statically or dynamically according to pre-defined rules.

3. The method according to claim 1 or 2,
   wherein the user-definable internal anonymization policy is configured per device instance and/or asset instance or based on anonymization policy rules based on properties of the device instance and/or asset instance.

4. The method according to one of the claims 1 to 3,
   wherein the user-definable internal anonymization policy is configured using machine learning.

5. The method according to one of the claims 1 to 4,
   wherein the user-definable internal anonymization policy may contain at least one of the following anonymization rules to be applied on exchanged data: value anonymization rules, history-limit rules, identity anonymization rules, context anonymization rule.

6. The method according to one of the claims 1 to 5,
   further comprising the step of adjusting the user-definable internal anonymization policy dynamically.

7. A method for deanonymization and negotiation for predictive maintenance, the method comprising:

   - Receiving (S21), by a condition prediction service module (210), the anonymized data from a transmitting module (130);
   - Deanonymizating (S22), by an deanonymization module (220), the received and anonymized data using a user-definable internal deanonymization policy to generate deanonymized data; and
   - Providing (S23), by a quality estimation service module (230), prediction service based on the deanonymized data to generate predicition data.

8. The method according to claim 7,
   wherein the user-definable internal deanonymization policy is configured per device instance and/or asset instance or based on deanonymization policy rules based on properties of the device instance and/or asset instance.

9. The method according to one of the claims 7 to 8,
   wherein the user-definable internal deanonymization policy is configured using machine learning.

10. The method according to one of the claims 7 to 9,
    wherein the user-definable internal deanonymization policy may contain at least one of the following deanonymization rules to be applied on exchanged data: value deanonymization rules, history-limit rules, identity deanonymization rules, context deanonymization rule.

11. The method according to one of the claims 7 to 10,
    further comprising the step of adjusting the user-de-

finable internal deanonymization policy dynamically.

12. A system (100) for anonymization and negotiation for predictive maintenance the system comprising:

- an aggregation service module (110) configured to aggregate runtime data and/or context data using an aggregation policy to generate aggregated data;
- an anonymization module (120) configured to anonymizate the aggregated data using a user-definable internal anonymization policy to generate anonymized data; and
- a transmitting module (130) configured to send the anonymized data to a condition prediction service module (210).

13. A system (200) for deanonymization and negotiation for predictive maintenance, the system comprising:

- a condition prediction service module (210) configured to receive the anonymized data from a transmitting module (130);
- an deanonymization module (220) configured to deanonymizate the anonymized data using a user-definable internal deanonymization policy to generate deanonymized data; and
- a quality estimation service module (230) configured to provide prediction service based on the deanonymized data to generate predicition data

14. A network for predictive maintenance, the network comprising the system (100) according to claim 12 and the system (200) according to claim 13.

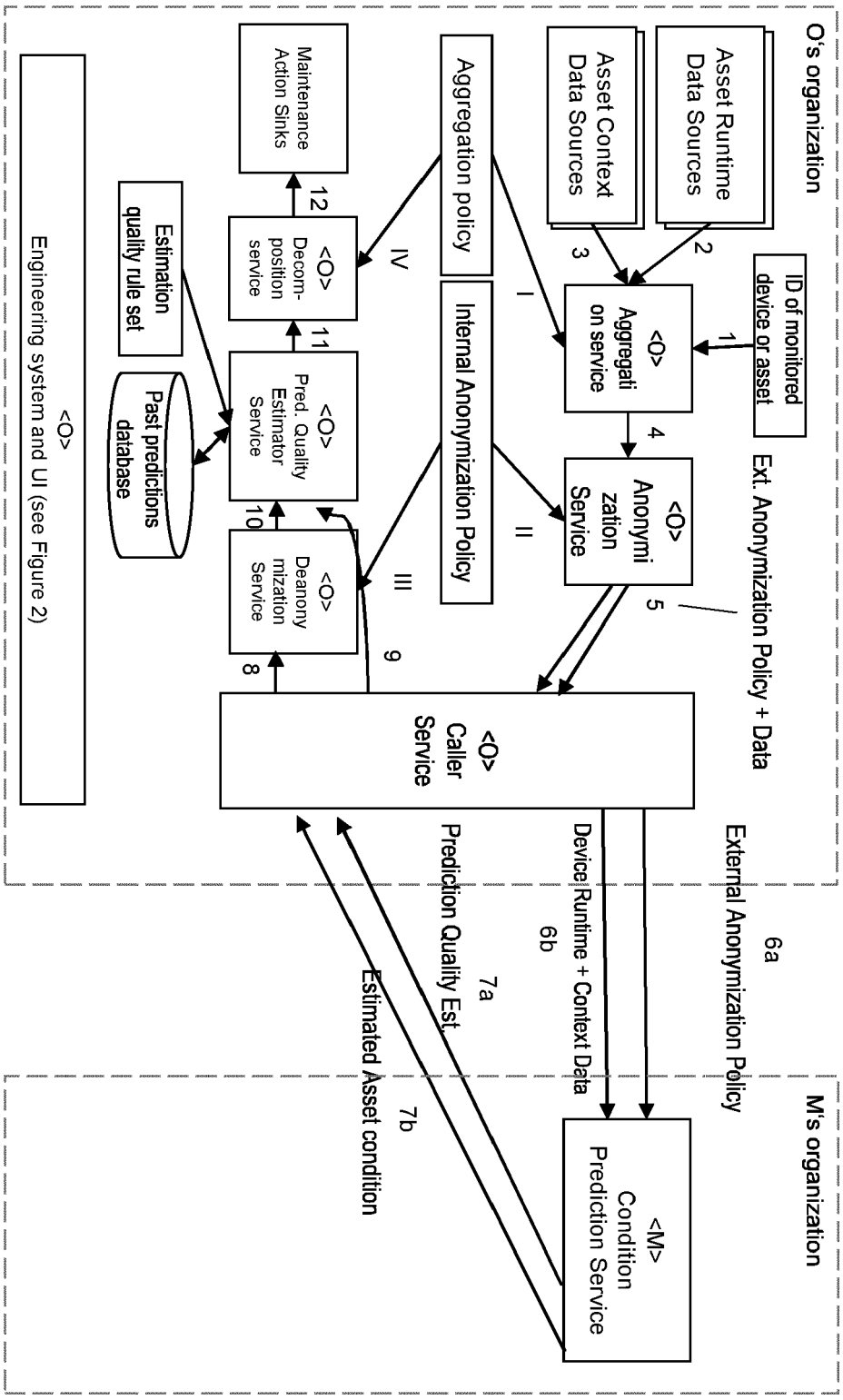
O's organization
Asset Runtime Data Sources
Asset Context Data Sources
ID of monitored device or asset
<O> Aggregation service
Aggregation policy
Internal Anonymization Policy
<O> Anonymization Service
Ext. Anonymization Policy + Data
<O> Caller Service
<O> Deanonymization Service
<O> Pred. Quality Estimator Service
<O> Decomposition service
Maintenance Action Sinks
Estimation quality rule set
Past predictions database
<O> Engineering system and UI (see Figure 2)
External Anonymization Policy
Device Runtime + Context Data
Prediction Quality Est.
Estimated Asset condition
M's organization
<M> Condition Prediction Service
1
2
3
4
5
6a
6b
7a
7b
8
9
10
11
12
I
II
III
IV

Fig. 1

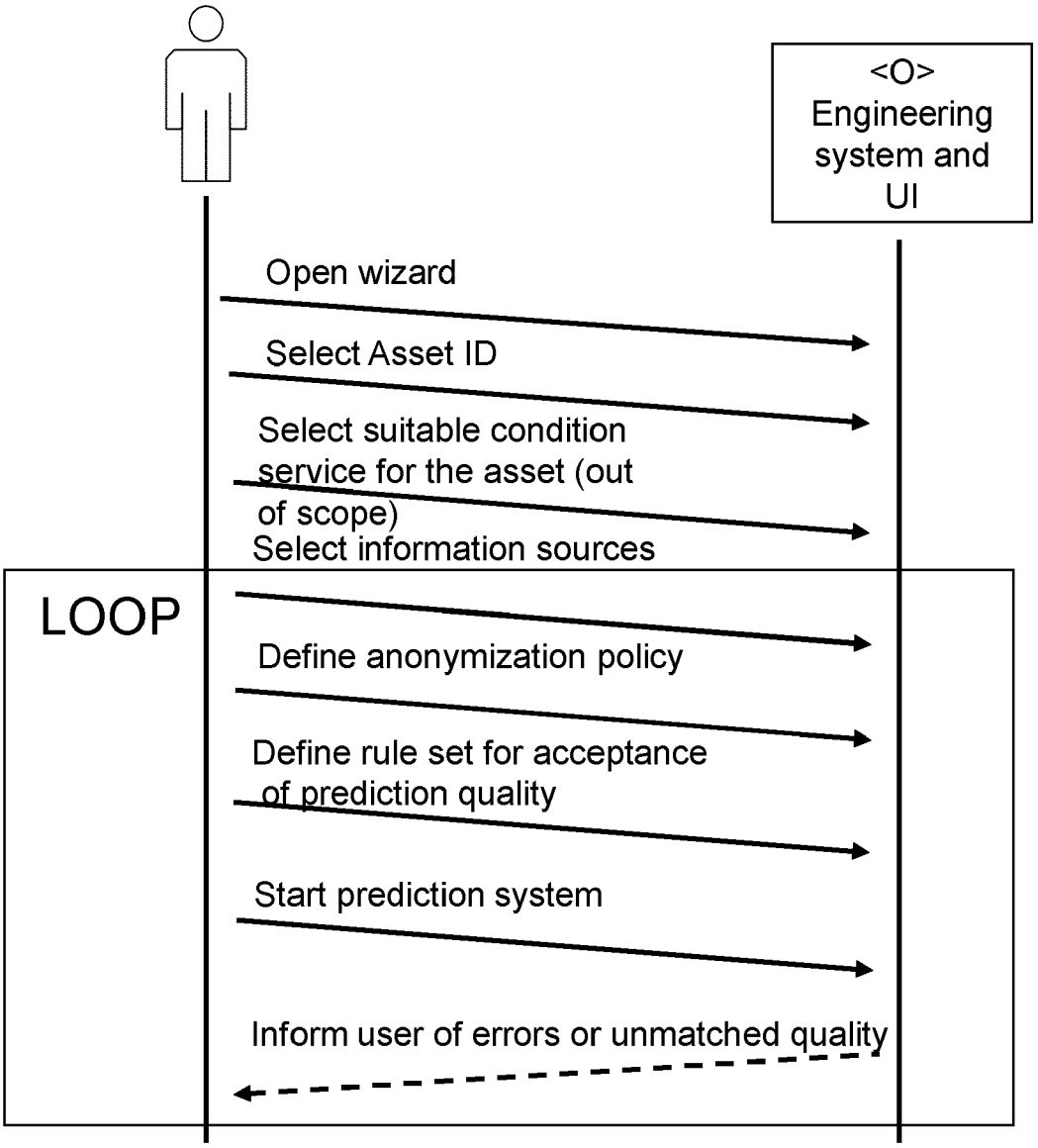
<O>
Engineering system and UI
Open wizard
Select Asset ID
Select suitable condition service for the asset (out of scope)
Select information sources
LOOP
Define anonymization policy
Define rule set for acceptance of prediction quality
Start prediction system
Inform user of errors or unmatched quality

Fig. 2

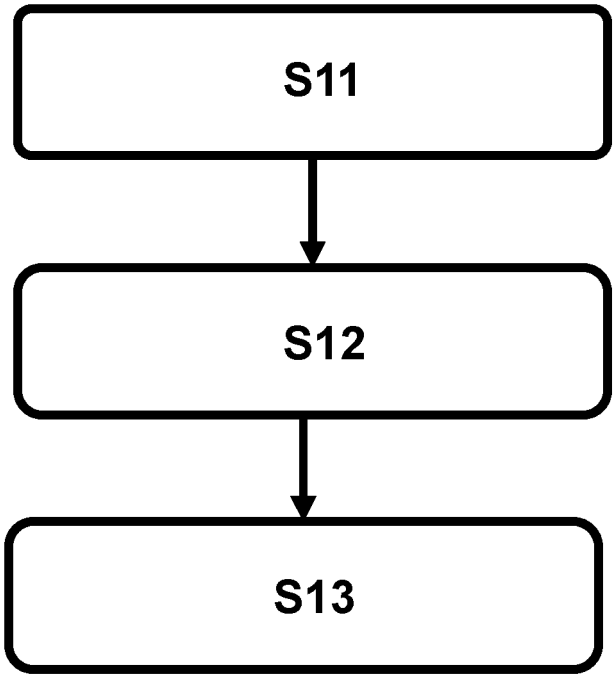

Fig. 3

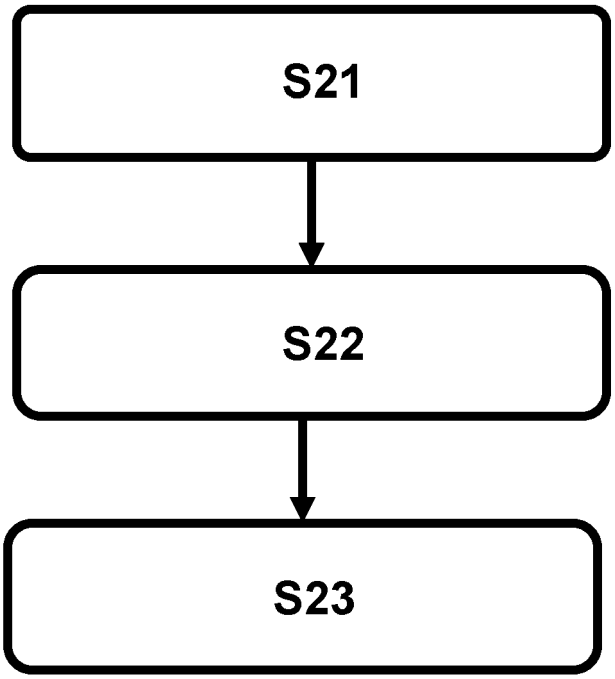

Fig. 4

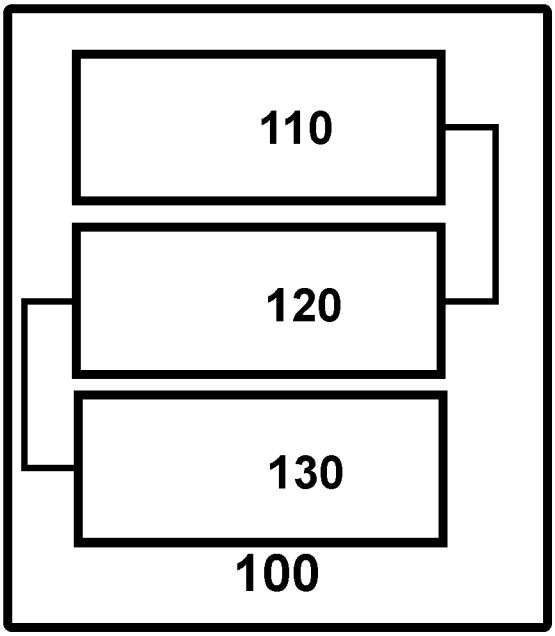

Fig. 5

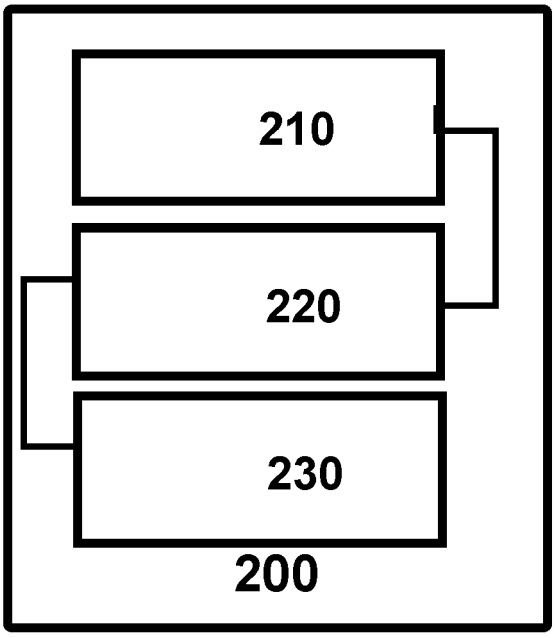

Fig. 6

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 22 17 8672

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2014/074730 A1 (ARENSMEIER JEFFREY N [US] ET AL) 13 March 2014 (2014-03-13) * claims 33-35 * * paragraph [0025] * * paragraph [0056] - paragraph [0060] * * paragraph [0233] - paragraph [0234] *	1-14	INV. G05B23/02 G06Q10/00
X	US 2014/336791 A1 (ASENJO JUAN L [US] ET AL) 13 November 2014 (2014-11-13) * paragraph [0067] * * paragraph [0070] * * paragraph [0073] * * paragraph [0097] * * paragraph [0105] *	1-14	
X	US 2019/372859 A1 (MERMOUD GRÉGORY [CH] ET AL) 5 December 2019 (2019-12-05) * paragraph [0063] - paragraph [0065] * * paragraph [0074] * * claims 1,5 *	1-14	
X	YU NANPENG ET AL: "Big data analytics in power distribution systems", 2015 IEEE POWER & ENERGY SOCIETY INNOVATIVE SMART GRID TECHNOLOGIES CONFERENCE (ISGT), IEEE, 18 February 2015 (2015-02-18), pages 1-5, XP032787899, DOI: 10.1109/ISGT.2015.7131868 [retrieved on 2015-06-23] * Section IV B. How to Control Privacy Risks in Deployment of Big Data Analytics in Power Distribution Systems *	1-14	TECHNICAL FIELDS SEARCHED (IPC) G05B G06Q
A	EP 3 203 679 A1 (ABB SCHWEIZ AG [CH]) 9 August 2017 (2017-08-09) * paragraph [0004] - paragraph [0005] *	1-14	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	7 November 2022	Aguilar, José María

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 22 17 8672

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	EP 3 461 054 A1 (UNIV VIGO [ES]) 27 March 2019 (2019-03-27) * paragraph [0012] - paragraph [0013] *	1-14	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	7 November 2022	Aguilar, José María

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 22 17 8672

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-11-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014074730 A1	13-03-2014	AU 2013225926 A1	18-09-2014
		CA 2865697 A1	06-09-2013
		CN 104272034 A	07-01-2015
		US 2014074730 A1	13-03-2014
		US 2018130031 A1	10-05-2018
		WO 2013130799 A1	06-09-2013
US 2014336791 A1	13-11-2014	CN 104142664 A	12-11-2014
		EP 2801938 A1	12-11-2014
		US 2014336791 A1	13-11-2014
US 2019372859 A1	05-12-2019	US 2019372859 A1	05-12-2019
		US 2020099590 A1	26-03-2020
EP 3203679 A1	09-08-2017	EP 3203679 A1	09-08-2017
		EP 3412000 A1	12-12-2018
		US 2018349740 A1	06-12-2018
		WO 2017134269 A1	10-08-2017
EP 3461054 A1	27-03-2019	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 3412000 A1 **[0042]**